Docket No.: 58895/P004US/10306553
(PATENT)

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In re Patent Application of:
Robert E. Cavanaugh

Application No.: 10/687,413 Confirmation No.: 8593

Filed: October 16, 2003 Art Unit: 2431

For: SYSTEMS AND METHODS FOR PROVIDING NETWORK SECURITY WITH ZERO NETWORK FOOTPRINT Examiner: S. H. Chen

# APPEAL BRIEF

MS Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Commissioner:

As required under 37 C.F.R. § 41.37(a), this brief is filed within two months of the Notice of Appeal filed in this case on September 11, 2009, and is in furtherance of said Notice of Appeal.

The fees required under 37 C.F.R. § 41.20(b)(2) are dealt with in the accompanying TRANSMITTAL OF APPEAL BRIEF.

This brief contains items under the following headings as required by 37 C.F.R. § 41.37 and M.P.E.P. § 1206:

IX. Evidence Appendix
X. Related Proceedings Appendix

## I. REAL PARTY IN INTEREST

The real party in interest for this appeal is:

Deep Nines Incorporated, a Texas corporation

## II. RELATED APPEALS, INTERFERENCES, AND JUDICIAL PROCEEDINGS

There are no other appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in this appeal.

## III. STATUS OF CLAIMS

### A. Total Number of Claims in Application

There are 17 claims pending in the application.

### B. Current Status of Claims

1. Claims canceled: 9, 10, 17-27, 31-35
2. Claims withdrawn from consideration but not canceled: None
3. Claims pending: 1-8, 11-16, 28-30
4. Claims allowed: None
5. Claims rejected: 1-8, 11-16, 28-30

### C. Claims On Appeal

The claims on appeal are claims 1-8, 11-16, 28-30.

## IV. STATUS OF AMENDMENTS

Appellant filed an Amendment After Final Rejection on August 28, 2009 canceling claims 17-27 and 31-35. The Examiner responded to the Amendment After Final Rejection

in an Advisory Action mailed September 9, 2009. The claims in the Claims Appendix incorporate the amendments indicated in the paper filed by Appellant on August 28, 2009.

## V. SUMMARY OF CLAIMED SUBJECT MATTER

A concise explanation of the subject matter defined in each of the claims separately argued in this appeal, which refers to the specification and to the drawings by reference characters, is provided below. All references to the specification and drawings are made by way of example for the convenience of the Board, as it is possible that other areas of the specification and drawings may contain further descriptive material. No limitations on the meaning of the following claim language is intended.

According to claim 1, a security system for use in conjunction with data flowing from a first device (*e.g.*, 11 of FIGURE 1) to a second device (*e.g.*, 12 of FIGURE 1) being directed to the second device in accordance with a network address of the second device includes a security device (*e.g.*, 100 of FIGURE 1) connected between the first and second devices, the security device accepting packet data for bridging to the second device, the security device operable for observing data flowing from the first device to the second device, the security device not itself having a network address or a physical address, and configured to be inserted between the first and the second device while a network connection is active (*e.g.*, page 2, lines 16-18; page4, line 21 – page 5, line 16; page 5, lines 27-29).

According to claim 8, a security device for use in a packet data network (*e.g.*, 101, 110 of FIGURE 1) where packets are delivered from a sending location (*e.g.*, 11 of FIGURE 1) to a destination location (*e.g.*, 12 of FIGURE 1) based upon one or more destination network addresses associated with each packet includes at least one NIC card (*e.g.*, 103 of FIGURE 1) for receiving data packets (*e.g.*, page 4, line 22 – page 5, line 4); a database (*e.g.*, 17 of FIGURE 1) for maintaining a list of destination network addresses to be secured by the device (*e.g.*, page 5, lines 17-18); wherein the at least one NIC card is connected to the network at any point between a sending location and one or more destination locations, the NIC card maintained in promiscuous mode such that the security device can observe all data directed to any destination addresses maintained from time to time in the list (*e.g.*, page 4, line 22 – page 5, line 4; page 5, lines 27-29); wherein the security device is connected to the network without establishing a network address or a physical address for the security device

(*e.g.*, page 2, lines 9-15; page 4, line 22 – page 5, line 4) ; and wherein the security device can be moved from location to location on the network without changing any network settings (*e.g.*, page 2, lines 17-19; page 5, lines 23-26).

According to claim 28, a security device (*e.g.*, 100 of FIGURE 1) for connection in a data network (*e.g.*, 101, 110 of FIGURE 1) ahead of a plurality of data destinations (*e.g.*, 12 of FIGURE 1) to be protected, each the destination identifiable by a unique network address includes means (*e.g.*, 13, 14, 103, 104, 100, 41, 410, 414, 415, 419, 411 of FIGURES 1, 3, and 4) for accepting data packets from the network without the data packets being addressed to the security device, the security device not including a physical address (*e.g.*, page 2, lines 9-15; page 4, line 21 – page 5, line 16; page 5, lines 27-29; page 8, line 8 – page 9, line 5; page 9, line 27 – page 10, line 5); and means (*e.g.*, 13, 14, 103, 104, 100, 41, 410, 414, 415, 419, 411 of FIGURES 1, 3, and 4) for passing accepted data packets to particular ones of the data destinations in accordance with destination addresses of the destinations to be detected and maintained for the security device (*e.g.*, page 2, lines 9-15; page 4, line 21 – page 5, line 16; page 5, lines 27-29; page 8, line 8 – page 9, line 5; page 9, line 27 – page 10, line 5).

## VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

The ground of rejection to be reviewed on appeal is as follows:

First Ground of Rejection – Claims 1-8, 11-16, 28-30 are rejected under 35 U.S.C. § 102(e) as being anticipated by US 2003/0229809 (hereinafter *Wexler*).

## VII. ARGUMENT

First Ground of Rejection – 35 U.S.C. § 102(e) Rejection (*Wexler*)

Claims 1-8, 11-16, 28-30 are rejected under 35 U.S.C. § 102(e) as being anticipated by *Wexler*. Appellant respectfully requests that the rejection be reversed at least because of the reasons articulated below.

To anticipate a claim under 35 U.S.C. § 102, a reference must teach every element of the claim. *E.g.*, *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). Moreover, in order for an applied reference to be

anticipatory under 35 U.S.C. § 102 with respect to a claim, "[t]he identical invention must be shown in as complete detail as is contained in the . . . claim." *Richardson v. Suzuki Motor Co.*, 9 U.S.P.Q.2d 1913, 1920 (Fed. Cir. 1989). As discussed further below, these requirements are not satisfied by the 35 U.S.C. § 102 rejection because *Wexler* does not teach every element of the claims.

Claims 1-7

Claim 1 recites, in part, "said security device not itself having a network address or a physical address." *Wexler* does not teach this feature of claim 1 at least because it does not appear to teach a security device not having a physical address. The Final Action cites *Wexler*'s proxy server 22 as teaching the claimed security device. Final Action at 2. However, *Wexler* teaches that its proxy server includes a MAC address, which is one type of physical address—"[i]f the requested address is included in the cache, transparency module 46 responds by transmitting (154) an ARP response which includes the MAC address of the port of proxy server 22 through which the request was received." *Wexler* at [0105] (emphasis added). Accordingly, *Wexler* fails to teach the above-recited feature of claim 1 because Wexler explicitly teaches that its proxy server 22 includes a MAC address.

For this reason alone, regardless of any other arguments made by the Examiner, the rejection must be reversed. Nevertheless, in the interest of completeness, Appellant addresses the Examiner's other reasoning.

In response to Applicant's arguments, the Final Action cites paragraph [0048] of *Wexler*, which states, in part, "[o]ptionally, edge router 26 and/or external router 28 are not aware of the presence of proxy server 22 along path 24, in layer-2." Final Action at 2-3 and 13. The Final Action alleges that the above-quoted sentence of *Wexler* teaches that *Wexler*'s proxy server may not include a layer-2 address and, thus, *Wexler* teaches an embodiment not having a physical address. The rejection struggles with having to reconcile *Wexler*'s explicit statement that the proxy server 22 has a MAC address with the sentence in paragraph [0048] that says that routers 26 and 28 may not be aware of the level-2 presence of the proxy server 28.

The above-quoted sentence from paragraph [0048] of *Wexler* does not say that the proxy server 22 does not have a physical address. Rather, paragraph [0048] of *Wexler* says that routers 26 and 28 may not be aware of the presence of proxy server 22 in level-2. The rejection assumes that lack of awareness of a level-2 address by routers 26 and 28 necessarily means that proxy server 22 does not have a level-2 address, but the assumption is incorrect, and the rejection fails.

The context of the above-quoted sentence indicates that proxy server 22 of *Wexler* does, indeed, have a level-2 address, but that its level-2 address is not indicated in forwarded packets. In the two sentences preceding the above-quoted sentence, *Wexler* describes actions by the proxy server 22 to keep its level-3 presence unknown. *Wexler* explains that proxy server 22 forwards packets with the same IP addresses "as they are received," so that router 26 and router 28 are not aware of the presence of proxy server 22 in level-3. *Wexler* at [0048]. The sentence cited by the Final Action implies an operation similar to the level-3 operation that keeps the level-2 presence of the proxy server 22 unknown by forwarding packets with the same addresses as are in the received packets.

In other words, *Wexler* teaches that proxy server 22 has a level-2 address, but also that packets forwarded by proxy server 22 do not provide other components with an indication of the level-2 address of proxy server 22. Appellant's explanation of paragraph [0048] is consistent with other teachings in *Wexler*. By contrast, the Examiner's interpretation of paragraph [0048] is contradicted by explicit teachings in *Wexler* at paragraph [0105] that proxy server 22 has a MAC address. Accordingly, it is clear that *Wexler* does not teach "said security device not itself having a network address or a physical address," as recited by claim 1.

Dependent claims 2-7 each depend either directly or indirectly from independent claim 1 and, thus, inherit all of the limitations of independent claim 1. Thus, *Wexler* does not meet all claim limitations of claims 2-7. It is respectfully submitted that dependent claims 2-7 are allowable at least because of their dependence from claim 1 for the reasons discussed above. Accordingly, Appellant respectfully requests the reversal of the 35 U.S.C. § 102 rejection of claims 1-7.

Claims 8 and 11-16

Claim 8 recites, in part, "said security device is connected to said network without establishing a network address or a physical address for said security device." *Wexler* does not teach this feature of claim 8 at least because it does not appear to teach a security device not having a physical address. The Final Action cites *Wexler*'s proxy server 22 as teaching the claimed security device. Final Action at 5. However, *Wexler* teaches that its proxy server includes a MAC address, which is one type of physical address. *Wexler* at [0105].

In response to Applicant's arguments, the Final Action cites paragraph [0048] of *Wexler*, which states that routers 26 and 28 may not be aware of the presence of proxy server 22 in level-2. Final Action at 13. The rejection assumes that lack of awareness of a level-2 address by routers 26 and 28 necessarily means that proxy server 22 does not have a level-2 address, but the assumption is incorrect, and the rejection fails.

A review of cited paragraph [0048] reveals that *Wexler* teaches that proxy server 22 has a level-2 address, but also that packets forwarded by proxy server 22 do not provide other components with an indication of the level-2 address of proxy server 22. Accordingly, it is clear that *Wexler* does not teach "said security device is connected to said network without establishing a network address or a physical address for said security device," as recited by claim 8.

Dependent claims 11-16 each depend either directly or indirectly from independent claim 8 and, thus, inherit all of the limitations of independent claim 8. Thus, *Wexler* does not meet all claim limitations of claims 11-16. It is respectfully submitted that dependent claims 11-16 are allowable at least because of their dependence from claim 8 for the reasons discussed above. Accordingly, Appellant respectfully requests the reversal of the 35 U.S.C. § 102 rejection of claims 8 and 11-16.

Claims 28-30

Claim 28 recites, in part, "said security device not including a physical address." *Wexler* does not teach this feature of claim 28 at least because it does not appear to teach a security device not having a physical address. The Final Action cites *Wexler*'s proxy server

22 as teaching the claimed security device. Final Action at 10. However, *Wexler* teaches that its proxy server includes a MAC address, which is one type of physical address. *Wexler* at [0105].

In response to Applicant's arguments, the Final Action cites paragraph [0048] of *Wexler*, which states that routers 26 and 28 may not be aware of the presence of proxy server 22 in level-2. Final Action at 13. The rejection assumes that lack of awareness of a level-2 address by routers 26 and 28 necessarily means that proxy server 22 does not have a level-2 address, but the assumption is incorrect, and the rejection fails.

A review of cited paragraph [0048] reveals that *Wexler* teaches that proxy server 22 has a level-2 address, but also that packets forwarded by proxy server 22 do not provide other components with an indication of the level-2 address of proxy server 22. Accordingly, it is clear that *Wexler* does not teach "said security device not including a physical address," as recited by claim 28.

Dependent claims 29 and 30 each depend either directly or indirectly from independent claim 28 and, thus, inherit all of the limitations of independent claim 28. Thus, *Wexler* does not meet all claim limitations of claims 29 and 30. It is respectfully submitted that dependent claims 29 and 30 are allowable at least because of their dependence from claim 28 for the reasons discussed above. Accordingly, Appellant respectfully requests the reversal of the 35 U.S.C. § 102 rejection of claims 28-30.

## VIII. CLAIMS APPENDIX

A copy of the claims involved in the present appeal is attached hereto as the Claims Appendix.

## IX. EVIDENCE APPENDIX

No evidence pursuant to §§ 1.130, 1.131, or 1.132 or entered by or relied upon by the examiner is being submitted.

## X. RELATED PROCEEDINGS APPENDIX

No related proceedings are referenced in II. above, hence copies of decisions in related proceedings are not provided.

Dated: November 11, 2009

Respectfully submitted,

By_____

Thomas Kelton
Registration No.: 54,214
FULBRIGHT & JAWORSKI L.L.P.
2200 Ross Avenue, Suite 2800
Dallas, Texas 75201-2784
(214) 855-7115
(214) 855-8200 (Fax)
Attorney for Appellant

## CLAIMS APPENDIX

The claims on appeal are as follows:

1. A security system for use in conjunction with data flowing from a first device to a second device being directed to said second device in accordance with a network address of said second device, said system comprising:

a security device connected between said first and second devices, said security device accepting packet data for bridging to said second device, said security device operable for observing data flowing from said first device to said second device, said security device not itself having a network address or a physical address, and configured to be inserted between said first and said second device while a network connection is active.

2. The security system of claim 1 wherein said first device could be any device on the unsecured side of said security device, each said first device having a unique network address, and wherein said second device could be any device on the secured side of said security device, each said second device having a unique network address.

3. The security system of claim 2 wherein said security device maintains a list of addresses for which it has security responsibility and wherein said security device only observes those data packets containing the network addresses maintained in said list.

4. The security system of claim 3 wherein said list includes addresses of both said first devices and said second devices.

5. The security system of claim 1 wherein said observing comprises:

a monitoring system for gathering information pertaining to the operation of said second device; and

a mechanism for modifying the flow of data into said security system depending upon said gathered information.

6. The security system of claim 5 wherein said gathered information is selected from the list containing:

number of arriving packets in a particular time interval;

the type of requests contained within given packets;

the nature of the informational content of the packets;

the sending identity of the packets;

the destination of the packets;

the traffic patterns formed by packets from specific sources;

the number of arriving packets from specific sources;

the correctness of the packets;

certain data contained in one or more messages; and

the type of file attached to a message.

7. The security system of claim 5 wherein said flow modifying mechanism operates to compare said gathered information with certain pre-established criteria and to set limits, and wherein said operational characteristics of said mechanism is modified in accordance with said set limits.

8. A security device for use in a packet data network where packets are delivered from a sending location to a destination location based upon one or more destination network addresses associated with each packet, said security device comprising:

at least one NIC card for receiving data packets;

a database for maintaining a list of destination network addresses to be secured by said device;

wherein said at least one NIC card is connected to said network at any point between a sending location and one or more destination locations, said NIC card maintained in promiscuous mode such that said security device can observe all data directed to any destination addresses maintained from time to time in said list;

wherein said security device is connected to said network without establishing a network address or a physical address for said security device; and

wherein said security device can be moved from location to location on said network without changing any network settings.

11. The security device of claim 8 further comprising:

a plurality of NIC cards all operating in said promiscuous mode.

12. The security device of claim 11 wherein said security device has a zero network footprint while said NIC cards are in said promiscuous mode.

13. The security device of claim 12 wherein all of said NIC cards share the same destination list.

14. The security device of claim 8 wherein said observing comprises:

monitoring system for gathering information pertaining to the operation of said second device; and

mechanism for modifying the flow of data into said security system depending upon said gathered information.

15. The security device of claim 14 wherein said gathered information is selected from the list containing:

number of arriving packets in a particular time interval;

the type of requests contained within given packets;

the nature of the informational content of the packets;

the sending identity of the packets;

the response destination of the packets;

the traffic patterns formed by packets from specific sources;

the number of arriving packets from specific sources;

certain data contained in one or more messages; and

the type of file attached to a message.

16. The security device of claim 15 wherein said flow modifying mechanism operates to compare said gathered information with certain pre-established criteria and to set limits, and wherein said operational characteristics of said gateway router are modified in accordance with said set limits.

28. A security device for connection in a data network ahead of a plurality of data destinations to be protected, each said destination identifiable by a unique network address, said security device comprising:

means for accepting data packets from said network without said data packets being addressed to said security device, said security device not including a physical address; and

means for passing accepted data packets to particular ones of said data destinations in accordance with destination addresses of said destinations to be detected and maintained for said security device.

29. The security device of claim 28 wherein said maintained destination addresses are stored in a database internal to said security device.

30. The security device of claim 28 wherein said accepting means comprises:

at least one network termination operating in a promiscuous mode.

## EVIDENCE APPENDIX

None.

## RELATED PROCEEDINGS APPENDIX

None.